JOURNAL OF ALGEBRA **179,** 808–837 (1996)
ARTICLE NO. 0038

Replication Formulae for $n \mid h$-Type Hauptmoduls

Charles R. Ferenbaugh

E-Systems, Garland Division, Dallas, Texas 75266-0023

Communicated by George Glauberman

Received October 18, 1994

1. INTRODUCTION

In the "Monstrous Moonshine" paper [CoN] Conway and Norton observed empirically that a modular function could be assigned to each conjugacy class of M in such a way that the Fourier coefficients of these functions were apparently characters of M. They also noticed that the power maps of Monster elements seemed to correspond to certain identities relating these functions; these identities came to be known as *replication formulae*. Later it was discovered that similar replication relations and power maps seemed to hold for a wider class of modular functions. At the time, all of these correspondences were conjectural.

In this paper we shall give a proof of the replication formulae and related results for a class of modular functions which we call $n \mid h$*-type*; this class includes all of the "Monstrous Moonshine" functions and many others as well.

Connections to other results. There is some overlap between the present paper and several other recent papers; here is a brief list of the related papers.

After I proved the results in this paper, I received a copy of Koike's preprint [Koi], which proves many of the same results. He proves that $n \mid h$-type functions are completely replicable, using a method of coset decompositions which can be shown equivalent to the lattice method used here. He also proves several of the same subsidiary results such as the compression formulae. Unfortunately, Koike's preprint does not seem to have been published even though it came out several years ago. (In [Fer2], I claimed that Koike's proof was incomplete. I now withdraw that claim; I had misread part of his preprint.)

The lattice presentation of the standard Hecke operator T_n described here is already well established in the literature; see [Ser], [Kob] for more details.

0021-8693/96 $12.00

A complete list of $n \mid h$-type groups of genus zero can be found in [Fer1]. This list also contains a variant sort of group in which some of the $+e$'s are replaced by $+\bar{e}$'s. These groups are also completely replicable, and satisfy suitably modified power-map rules and compression formulae; this can be proved by minor modifications of the proofs given here.

In the preprint [CuN], Cummins and Norton prove that all Hauptmoduls of a certain type are replicable (though not necessarily *completely* replicable). Their proof works for a much wider class of functions than this proof; however, they do not specify what the replicates are. For this reason, their proof cannot be used in Borcherds' construction of the Monster Lie algebra, as described below.

Finally, we mention the proof of the original Moonshine conjectures, which follows from Borcherds' construction in [Bor] of a Lie algebra acted on naturally by the Monster. The traces of these actions are some set of completely replicable functions, since they satisfy Norton's bivarial form of the replication formulae. Borcherds then uses the result of this paper or that of [Koi] that the modular functions $J_m(z)$, as listed explicitly in [CoN], are completely replicable. He verifies that the coefficients a_1, a_2, a_3, and a_5 of the two sets of functions are identical. As observed in [ACMS], any replicable function is completely determined by the values of a_1, a_2, a_3, and a_5 for itself and its replicates. So this is sufficient to prove that all of the a_n are identical, that is, that the Monster Lie algebra has as traces the functions $J_m(z)$.

(Note that this method works *only* if the replicates are known. Otherwise, coefficients up to a_{23} would need to be checked; see the appendix to [CuN].)

Overview. In Section 1, we summarize some background material, and prove a few simple results concerning modular groups. In Section 2, we work with Hauptmoduls of groups $\Gamma_0(N)$, defining and proving the replication formulae in terms of the twisted Hecke operator $\hat{T}_m$. We then extend these methods to general $n \mid h$-type groups in Section 3.

1.1. *Modular Groups and Hauptmoduls*

We begin with a brief review of some notation and results from [Fer1]. We consider subgroups of $PSL_2(\mathbf{R})$ of the form

$$\Gamma_0(n \mid h) = \left\langle \begin{pmatrix} a & b/h \\ cn & d \end{pmatrix} \middle| a, b, c, d \in \mathbf{Z}, ad - bcn/h = 1 \right\rangle$$

and

$$\Gamma_0(n \mid h) + e_1, e_2, \ldots = \langle \Gamma_0(n \mid h), w_{e_1}, w_{e_2}, \ldots \rangle,$$

where the w_e's are Atkin–Lehner involutions

$$w_e = \left\{ \begin{pmatrix} ae & b/h \\ cn & de \end{pmatrix} \middle| a, b, c, d \in \mathbf{Z}, ade^2 - bcn/h = e \right\}$$

and $\{e_0 = 1, e_1, e_2, \ldots\}$ is a subgroup of $\mathrm{Ex}(n/h)$, the group of exact, or Hall, divisors of n/h under the operation $e * e' = ee'/(e, e')^2$. When $h = 1$, we simplify the notation by writing $\Gamma_0(N)$ or $\Gamma_0(N)-$ for the base group, and W_E for the Atkin–Lehner involutions. We write Γ to denote the group $\Gamma_0(1) = PSL_2(\mathbf{Z})$.

We shall restrict our attention to groups for which $h \mid 24$; in this case $\Gamma_0(n \mid h) + e_1, e_2, \ldots$ normalizes $\Gamma_0(N)$, where $N = nh$. (See [CoN] for more details on this.)

Next, we define a homomorphism λ: $\Gamma_0(n \mid h) + e_1, e_2, \ldots \to \mathbf{C}^*$ as follows:

1. $\lambda = 1$ for elements of $\Gamma_0(N)$, where $N = nh$;

2. $\lambda = 1$ for all the Atkin–Lehner involutions W_E of $\Gamma_0(N)$ (except when E has a prime divisor not dividing n/h);

3. $\lambda = e^{-2\pi i/h}$ for the coset containing $\left(\begin{smallmatrix} 1 & 1/h \\ 0 & 1 \end{smallmatrix}\right)$;

4. $\lambda = e^{\pm 2\pi i/h}$ for the coset containing $\left(\begin{smallmatrix} 1 & 0 \\ n & 1 \end{smallmatrix}\right)$, where the sign is $+$ if $z \mapsto -1/Nz$ is present, $-$ if not.

The kernel of λ is a normal subgroup of index h, denoted $(1/h)\Gamma_0(n \mid h) + e_1, e_2, \ldots$. We call such modular groups *$n \mid h$-type groups*.

Finally, we define a *Hauptmodul* of a modular group G to be a meromorphic bijection f: $\widehat{\mathbf{H}^+/G} \to \hat{\mathbf{C}}$. Such an f is a generator for the field of functions invariant under G. Furthermore, the groups we encounter will always contain the map $z \mapsto z + 1$. This implies that $f(z)$ can be written as a Fourier series in terms of $q = e^{2\pi i z}$, and that it can be normalized to the form

$$q^{-1} + 0 + a_1 q + a_2 q^2 + \cdots .$$

We shall call such a function a *normalized* Hauptmodul.

In general, we shall use the symbol $J_{n \mid h + e_1, e_2, \ldots}(z)$ to denote the normalized Hauptmodul of $(1/h)\Gamma_0(n \mid h) + e_1, e_2, \ldots$. For any function f invariant under this group, we shall say f is of *type* $n \mid h + e_1, e_2, \ldots$.

1.2. *Moonshine and Replication*

In [CoN], Conway and Norton made the following conjecture:

PROPOSITION 1.1 ("Monstrous Moonshine" conjecture). *To each element m of the Monster M we may assign a certain modular function $J_m(z)$, in*

such a way that the Fourier coefficients $a_k(m)$ given by

$$J_m(z) = q^{-1} + 0 + a_1(m)q + a_2(m)q^2 + \cdots \qquad (q = e^{2\pi iz})$$

are in fact characters of M. Furthermore, the function $J_m(z)$ is always the normalized Hauptmodul for some modular group $(1/h)\Gamma_0(n \mid h) + e_1, e_2, \ldots$ of genus zero, where n is the order of the element m. We call this group the fixing group $F(m)$.

The functions $J_m(z)$ are given by an explicit list in [CoN] or [Fer1]. As noted in the Introduction, this conjecture was eventually proved by Borcherds in [Bor].

Using these correspondences, Conway and Norton then observed empirically that the power maps for elements of M have the following simple expression:

PROPOSITION 1.2 (power-map rule). *If J_m is of type $n \mid h + e_1, e_2, \ldots$, then J_{m^a} is of type $n' \mid h' + e_1', e_2', \ldots$, where $n' = n/(n, a)$; $h' = h/(h, a)$; and $e_1', e_2', \ldots$ are the divisors of n'/h' among the numbers $e_1, e_2, \ldots$.*

Note in particular that $F(m^a) = F(m)$ whenever $(n, a) = 1$.

For general Monster elements m, Conway and Norton found *replication formulae* which seemed to relate $J_m(z)$ to its various powers $J_{m^a}(z)$ for all integers a. Later, in [ACMS], [FMN], it was discovered that many other modular functions $f(z)$ could be assigned *replicates* $f^{(a)}(z)$ which seemed to satisfy these formulae. In [FMN] it was noted that many of the non-Monstrous replicable functions could be described using the $n \mid h$ notation, and for these the same "power-map" rule held between the fixing groups $F(f)$ and $F(f^{(a)})$.

A complete list of all Hauptmoduls of these $n \mid h$-type, or *Monster-like*, groups can be found in [Fer1].

1.3. *Invariance Groups of Replicates*

We note here some useful properties of the fixing groups under consideration. These will be used later in the proof of the replication formulae. First we recall the following lemma (for a proof see [Fer1]):

LEMMA 1.3. *Let $(m, n) = 1$, and let $\left(\begin{smallmatrix} a & b/h \\ cn & d \end{smallmatrix}\right)$ be in $\Gamma_0(n \mid h)$. Then*:

1. *There exist a_1, b_1, c_1, d_1 such that $m \mid c_1$ and*

$$\begin{pmatrix} a_1 & b_1/h \\ c_1 n & d_1 \end{pmatrix} \equiv \begin{pmatrix} a & b/h \\ cn & d \end{pmatrix} \qquad (\mathrm{mod}\ \Gamma_0(N)).$$

2. *Similarly, but with* $m \mid b_1$ *instead of* $m \mid c_1$.

Let $F_1(f)$ denote the subgroup of $F(f)$ containing all elements with determinant 1. Then we can prove the following theorem:

THEOREM 1.4. *Suppose f is a Hauptmodul of type* $n \mid h + e_1, e_2, \ldots$.

1. *If* $p \nmid n$, *and if* $p \mid c$, *then*

$$\begin{pmatrix} a & b/h \\ cn & d \end{pmatrix} \in F_1(f) \Leftrightarrow \begin{pmatrix} a & bp/h \\ (c/p)n & d \end{pmatrix} \in F_1(f).$$

2. *If* $p \mid h$,

$$\begin{pmatrix} a & b/h \\ cn & d \end{pmatrix} \in F_1(f) \Rightarrow \begin{pmatrix} a & b/(h/p) \\ c(n/p) & d \end{pmatrix} \in F_1(f^{(p)}).$$

3. *If* $p \mid n$ *and* $p \nmid h$,

$$\begin{pmatrix} a & b/h \\ cn & d \end{pmatrix} \in F_1(f) \Leftrightarrow \begin{pmatrix} a & bp/h \\ c(n/p) & d \end{pmatrix} \in F_1(f^{(p)}).$$

Proof. Note that, in all three cases, the second matrix mentioned is simply the conjugate of the first by $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$. Let H_p denote this homomorphism. Let λ be the homomorphism used to define $F(f)$, and let $\zeta = e^{2\pi i/h}$.

In case 1, we have

$$\begin{array}{lll} & \Gamma_0(np \mid h) \overset{H_p}{\to} \Gamma_0(n \mid h) \overset{\lambda}{\to} C_h & \\ \lambda = \zeta^{-1} & \begin{pmatrix} 1 & 1/h \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & p/h \\ 0 & 1 \end{pmatrix} \mapsto \zeta^{-p} & \\ \lambda = \zeta^{\pm p} & \begin{pmatrix} 1 & 0 \\ np & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \mapsto \zeta^{\pm 1} & \\ \lambda = 1 & \Gamma_0(Np) \mapsto \Gamma_0(N, p) \mapsto 1. & \end{array}$$

So for the matrices γ in the left-hand column, we have $\lambda(H_p(\gamma)) = \lambda(\gamma)^p$ (noting that, since $p \nmid h$ and $h \mid 24$, we have $p^2 \equiv 1 \pmod{h}$). But these matrices generate $\Gamma_0(np \mid h)$, so this equality holds on all of $\Gamma_0(np \mid h)$. Thus $\lambda(H_p(\gamma)) = 1$ if and only if $\lambda(\gamma) = 1$, and case 1 is proved.

(Note: by Lemma 1.3 we may assume that $p \mid c$.)

Similarly in case 2:

$$\Gamma_0(n\,|\,h) \overset{H_p}{\to} \Gamma_0((n/p)\,|\,(h/p)) \overset{\lambda'}{\to} C_{h/p}$$

$$\lambda = \zeta^{-1} \qquad \begin{pmatrix} 1 & 1/h \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 1/(h/p) \\ 0 & 1 \end{pmatrix} \mapsto \zeta^{-p}$$

$$\lambda = \zeta^{\pm 1} \qquad \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ n/p & 1 \end{pmatrix} \mapsto \zeta^{\pm p}$$

$$\lambda = 1 \qquad \Gamma_0(N) \mapsto \Gamma_0(N/p, p) \mapsto 1,$$

where λ' is the defining homomorphism for $F(f^{(p)})$. This shows, similarly to case 1, that $\lambda'(H_p(\gamma)) = \lambda(\gamma)^p$ and thus $\lambda(\gamma) = 1$ implies $\lambda'(H_p(\gamma)) = 1$ (though in this case, unlike the preceding one, the reverse is not always true). This proves case 2.

Finally, in case 3 we have

$$\Gamma_0(n\,|\,h) \overset{H_p}{\to} \Gamma_0((n/p)\,|\,h) \overset{\lambda'}{\to} C_h$$

$$\lambda = \zeta^{-1} \qquad \begin{pmatrix} 1 & 1/h \\ 0 & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & p/h \\ 0 & 1 \end{pmatrix} \mapsto \zeta^{-p}$$

$$\lambda = \zeta^{\pm 1} \qquad \begin{pmatrix} 1 & 0 \\ n & 1 \end{pmatrix} \mapsto \begin{pmatrix} 1 & 0 \\ n/p & 1 \end{pmatrix} \mapsto \zeta^{\pm 1}$$

$$\lambda = 1 \qquad \Gamma_0(N) \mapsto \Gamma_0(N/p, p) \mapsto 1.$$

We assert that $\lambda'(H_p(\gamma))$ equals 1 exactly when $\lambda(\gamma)$ does. If $h = 1$ or 2 this is trivial. If $h \geq 3$, there are two possibilities:

1. $p \equiv 1 \pmod h$ and the same sign is taken at both choices. Then $\lambda'(H_p(\gamma))$ and $\lambda(\gamma)$ are always equal.

2. $p \equiv -1 \pmod h$ and opposite signs are taken. Then $\lambda'(H_p(\gamma))$ and $\lambda(\gamma)$ are complex conjugates.

Tables 1.1 and 1.2 of [Fer1] contain a complete list of Hauptmoduls of $n\,|\,h$-type. By inspection, each of the $h \geq 3$ groups listed satisfies one of these two cases. This completes the proof. ∎

Note that property 3 of this theorem does not hold for arbitrary $n\,|\,h$-type groups, such as $24\,|\,4-$ with $p = 3$. So our reference to the list of Hauptmoduls in [Fer1] is a necessary part of the proof.

By combining properties 1 and 3 of the above result, we have:

COROLLARY 1.5. *If $p \nmid h$, then $F_1(f) \subseteq F_1(f^{(p)})$.*

In the $p\,|\,h$ case, we can establish a related result:

LEMMA 1.6. *With notation as above, if $p\,|\,h$, then $H_p(F_1(f))$ and $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ generate $F_1(f^{(p)})$.*

Proof. Suppose $\gamma \in F_1(f^{(p)})$. By Lemma 1.3, we can find a β such that $\gamma = H_p(\beta)$. Now $\lambda'(\gamma) = 1$. We saw in the proof of Theorem 1.4 that $\lambda'(H_p(\beta)) = \lambda(\beta)^p$, so $\lambda(\beta)$ must be a pth root of unity. Let

$$\delta = \begin{pmatrix} 1 & 1/p \\ 0 & 1 \end{pmatrix}.$$

Then $\lambda(\delta) = e^{-2\pi i/p}$, so we may pick an integer k such that $\lambda(\delta^{-k}\beta) = 1$. Then $\delta^{-k}\beta \in F_1(f)$ and

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^k H_p(\delta^{-k}\beta) = \gamma.$$

Since γ was arbitrary this completes the proof. ∎

2. REPLICATION ON $\Gamma_0(N)$

In this section we will state the replication formulae, and develop the tools necessary to prove these formulae in the case where f is the Hauptmodul J_{N-} for $\Gamma_0(N)$. In some cases this can be done easily using the familiar Hecke operators T_m from the theory of modular functions, which restate certain sums of f's in terms of functions on lattices. We then develop a natural definition for the twisted Hecke operator $\hat{T}_m$, which can be used to express and prove the replication formulae in all cases.

Some of this material is patterned after Section VII.4 in [Ser]; also compare Section III.5 of [Kob]. A more expository presentation of these results can be found in [Fer2].

2.1. *Lattices and Modular Functions*: *Some Preliminaries*

We begin by characterizing $\Gamma_0(N)$ in terms of lattices:

PROPOSITION 2.1. *Given any lattice $L_1 \subset \mathbf{C}$ with basis ω_1, ω_2, let $L_N = \langle N\omega_1, \omega_2 \rangle$. Then*

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \middle| a, b, c, d \in \mathbf{Z}, \langle a\omega_1 + b\omega_2, c\omega_1 + d\omega_2 \rangle = L_1, \right.$$
$$\left. \langle N(a\omega_1 + b\omega_2), c\omega_1 + d\omega_2 \rangle = L_N \right\}.$$

This motivates the following definition:

DEFINITION 2.2. For any positive integer N, a *lattice pair of type N* is an ordered pair of lattices (L_1, L_N) such that $L_N \subseteq L_1$ and $L_1/L_N \cong C_N$. A basis for (L_1, L_N) is a pair of elements $\omega_1, \omega_2 \in \mathbf{C}$ such that $L_1 =$

$\langle \omega_1, \omega_2 \rangle$ and $L_N = \langle N\omega_1, \omega_2 \rangle$, and such that ω_1/ω_2 is in the upper halfplane $\mathbf{H}^+$.

Such a basis can always be chosen, by the structure theorem for finitely generated abelian groups; and the $\mathbf{H}^+$ condition can be met by replacing ω_1 by $-\omega_1$ if necessary.

DEFINITION 2.3. Given a lattice pair (L_1, L_N) of type N, for any $k \mid N$ we define $\mathrm{Ind}_k(L_1, L_N)$ to be the unique lattice L_k such that $L_N \subseteq L_k \subseteq L_1$ and $[L_1, L_k] = k$.

PROPOSITION 2.4. *There is a one-to-one correspondence between*:

1. *complex-valued functions F on lattice pairs of type N which have the* scalar multiplication property

$$F(\lambda L_1, \lambda L_N) = F(L_1, L_N)$$

for all lattice pairs (L_1, L_N) *and all* $\lambda \in \mathbf{C}^*$; *and*

2. *functions* $f\colon \mathbf{H}^+ \to \mathbf{C}$ *invariant under* $\Gamma_0(N)$.

Sketch of proof. Suppose we are given a function $f(z)$ invariant under $\Gamma_0(N)$. Then, for any lattice pair (L_1, L_N) of type N, we can define

$$F(L_1, L_N) = f\left(\frac{\omega_1}{\omega_2}\right),$$

where ω_1, ω_2 is a basis for (L_1, L_N). Then F is independent of our choice of basis, since f is invariant under $\Gamma_0(N)$.

Conversely, given $F(L_1, L_N)$, we define $f(z) = F(\langle z, 1\rangle, \langle Nz, 1\rangle)$. Then f can be shown invariant under $\Gamma_0(N)$, using the fact that f depends only on L_1 and L_N. For more details see [Kob]. ∎

2.2. *Hecke Operators*

Given any positive integer N, define the $\mathbf{Q}$-vector space X_N to be the set of all formal $\mathbf{Q}$-linear combinations of lattice pairs of type N, and define

$$\hat{X}_N = \bigoplus_{n \mid N} X_n.$$

Then any linear operator on X_N or $\hat{X}_N$ can be defined by giving its values at each lattice pair.

DEFINITION 2.5. For any $m \in \mathbf{Z}^+$, the twisted (or generalized) Hecke operator $\hat{T}_m$ is defined on $\hat{X}_N$ by

$$\hat{T}_m(L_1, L_N) = \frac{1}{m} \sum_{[L_1 : L'] = m} (L', L' \cap L_N).$$

The *twisted homothety operator* $\hat{R}_l$ for $l \in \mathbf{Z}^+$ is defined by

$$\hat{R}_l(L_1, L_N) = \frac{1}{l^2}(lL_1, lL_1 \cap L_N).$$

Note that, for any lattice $L' \subset L_1$, we have $L'/(L' \cap L_N) \cong C_n$ for some $n \mid N$, so $\hat{T}_m$ and $\hat{R}_l$ are in $\hat{X}_N$. Note also that, if we add the condition $L'/(L' \cap L_N) \cong C_N$ to the sum in $\hat{T}_m$, the definition becomes that of the standard Hecke operator T_m as given in [Kob].

We can then state the following proposition, which is a generalization of proposition VII.5.10 of [Ser]. (The proof is analogous to Serre's, and will not be repeated here.)

PROPOSITION 2.6. *Our operators $\hat{R}_l$ and $\hat{T}_n$ satisfy the identities*

$$\hat{R}_l\hat{R}_m = \hat{R}_{lm} \qquad \text{for } l, m \in \mathbf{Z}$$

$$\hat{R}_l\hat{T}_n = \hat{T}_n\hat{R}_l \qquad \text{for } l, n \in \mathbf{Z}$$

$$\hat{T}_m\hat{T}_n = \hat{T}_{mn} \qquad \text{if } (m, n) = 1$$

$$\hat{T}_p\hat{T}_{p^n} = \hat{T}_{p^{n+1}} + p\hat{T}_{p^{n-1}}\hat{R}_p \qquad \text{for } p \text{ prime}, n \geq 1.$$

Equivalently, we can express later $\hat{T}_m$ in terms of earlier ones:

COROLLARY 2.7. *Suppose $p \mid m$ for some prime p. Then*

$$\hat{T}_m = \begin{cases} \hat{T}_p\hat{T}_{m/p} & \text{if } p \parallel m \\ \hat{T}_p\hat{T}_{m/p} - p\hat{T}_{m/p^2}\hat{R}_p & \text{if } p^2 \mid m. \end{cases}$$

Now suppose, for a function $f = J_{N-}$, we define its replicates $\{f^{(a)}\}$ according to the power-map rule. We can then easily verify the following two properties:

PROPOSITION 2.8. 1. *For any $n \mid N$, $f^{(n)}$ is invariant under $\Gamma_0(N/n)$.*

2. *For any a, $f^{(a)} = f^{(\gcd(a, N))}$. In other words, we have $f^{(a)} = f$ for all a relatively prime to N, and similarly for the replicates of f.*

By property 1, for any $n \mid N$, we may use $f^{(n)}$ to define a corresponding function F on lattice pairs of type N/n, and by $\mathbf{Q}$-linearity this extends to define F on all of $\hat{X}_N$.

Given such an f and its corresponding F, let A be any linear operator on $\hat{X}_N$. Then we define

$$(f \mid A)(z) = F(A(\langle z, 1\rangle, \langle Nz, 1\rangle)).$$

We can now find equivalent definitions for $f \mid \hat{T}_m$ and $f \mid \hat{R}_l$ which do not involve lattices. It is easily verified that

$$\left(l^2 f \mid \hat{R}_l\right)(z) = f^{(\gcd(l, N))}(z) = f^{(l)}(z).$$

The expression for $\hat{T}_m$ is derived using the following lemma, quoted from Section VII.5.2 of [Ser]:

LEMMA 2.9. *Given a lattice $L = \langle \omega_1, \omega_2 \rangle$ and an integer $m \geq 1$, any sublattice of index m in L can be expressed as $\langle a\omega_1 + b\omega_2, d\omega_2 \rangle$, where a, b, d are integers with $ad = m$ and $0 \leq b < d$. Each set of values of a, b, d gives a distinct sublattice.*

Using this lemma, we find that this definition of $\hat{T}_m$ is equivalent to that proposed in [ACMS]:

PROPOSITION 2.10.

$$\left(mf \mid \hat{T}_m\right)(z) = \sum_{\substack{ad = m \\ 0 \leq b < d}} f^{(a)}\left(\frac{az + b}{d}\right).$$

The *standard Hecke operator* $T_m(L_1, L_N)$ includes only those terms of $\hat{T}_m(L_1, L_N)$ which are lattice pairs of type N. In the language of modular functions, T_m contains only the terms of $\hat{T}_m$ that mention f itself, rather than some different $f^{(a)}$. Since $f^{(a)} = f$ exactly when $(a, N) = 1$, we have:

COROLLARY 2.11.

$$(mf \mid T_m)(z) = \sum_{\substack{ad = m,\ (a, N) = 1 \\ 0 \leq b < d}} f\left(\frac{az + b}{d}\right).$$

In particular, we note the following two special cases:

COROLLARY 2.12. *If $(m, N) = 1$, then $f \mid T_m = f \mid \hat{T}_m$.*

COROLLARY 2.13. *If p is a prime with $p \mid N$, then*

$$\left(pf \mid T_p\right)(z) = f\left(\frac{z}{p}\right) + f\left(\frac{z + 1}{p}\right) + \cdots + f\left(\frac{z + (p - 1)}{p}\right),$$

and

$$\left(pf \mid \hat{T}_p\right)(z) = f^{(p)}(pz) + \left(pf \mid T_p\right)(z).$$

It is clear that $F(T_m(L_1, L_N))$ and $F(\hat{T}_m(L_1, L_N))$ are invariant under any transformation which preserves L_1 and L_N. Restating this in terms of f gives:

PROPOSITION 2.14. 1. *For any m, and any f invariant under $\Gamma_0(N)$, the function $f \mid T_m$ is invariant under $\Gamma_0(N)$.*

2. *For any m, and any f satisfying Proposition* 2.8, *the function $f \mid \hat{T}_m$ is invariant under $\Gamma_0(N)$.*

2.3. *Replication for* Γ

The property of replicability can be expressed in several different ways. We use here the definition given in [ACMS].

DEFINITION 2.15. Given a Hauptmodul f with Fourier series $q^{-1} + \sum_{i=1}^{\infty} a_i q^i$, we define $P_m(f)$ to be the unique polynomial of degree m such that

$$P_m(f(z)) \cong q^{-m} \qquad (\mathrm{mod}\ q\mathbf{Z}[[q]]).$$

In this case we say $P_m(f)$ has *leading term* q^{-m}.

DEFINITION 2.16. A function f is called *replicable* if there exist functions $\{f^{(a)}\}$, called replicates of f, such that the *m-plication formula*

$$mf \mid \hat{T}_m = P_m(f)$$

holds for all positive integers m.

We shall refer to all such formulae collectively as the *replication formulae*, and we call a function *completely replicable* if it and all its replicates are replicable.

If f is a normalized Hauptmodul J_{N-}, we define the replicates of f by the power map rule given in Proposition 1.2. We shall show later that these replicates satisfy the replication formulae. Also, if $g = P_m(f)$, we shall define the replicate $g^{(a)}$ to be the corresponding polynomial $P_m(f^{(a)})$.

We can now prove the statement which was used in [CoN] as a prototype for the replication formulae:

PROPOSITION 2.17. *The function J is completely replicable, with $J^{(a)} = J$ for all $a \geq 1$.*

Proof. First we recall from Proposition 2.14 that $J \mid \hat{T}_m$ is invariant under Γ for all m. This shows that $(mJ \mid \hat{T}_m)(z)$ is some rational function of $J(z)$. Next we calculate the leading coefficients of the Fourier series for $mJ \mid \hat{T}_m$, and find it to have the form $q^{-m} + \sum_{i=1}^{\infty} a_i q^i$. Next we observe that J has no poles in the upper half-plane, and the same is true for each of the summands in $mJ \mid \hat{T}_m$. Finally, we note that the fundamental region for Γ has no cusps on the real line. So the only poles of $mJ \mid \hat{T}_m(z)$, modulo Γ, are at $z = \infty$. Thus $(mJ \mid \hat{T}_m)(z)$ is a polynomial in $J(z)$; and, from its Fourier series above, we see that it must be $P_m(J(z))$. ∎

Now suppose we replace J by J_{N-}. The first few steps in the above proof still work: $mf \mid \hat{T}_m$ has the correct invariance group; its Fourier series has the proper form; and it has no poles in $\mathbf{H}^+$. But when $N > 1$, the

fundamental region for $\Gamma_0(N)$ has cusps on the real line, and the summands of $mf \mid \hat{T}_m$ have poles on the real line as well. So we are forced to check whether these poles and cusps coincide. We will need additional techniques to do this checking; these techniques will be developed in the next few sections.

2.4. *Variable Substitutions*

Suppose we want to express the transformation $z \mapsto (az + b)/(cz + d)$ in terms of lattices. We can do this by letting the matrix $A = \left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ act on a basis ω_1, ω_2 for a lattice pair (L_1, L_N). This defines a lattice homomorphism α: $L_1 \mapsto L'$ for some lattice L'. In general, different choices of ω_1, ω_2 will give different homomorphisms α. However:

THEOREM 2.18. *Let (L_1, L_N) be a lattice pair of type N, and let A be a matrix. Then the action of A on (L_1, L_N) is independent of the chosen basis exactly when A is in the normalizer of $\Gamma_0(N)$.*

Proof. Let ω_1, ω_2 be a basis for (L_1, L_N), and let α be the action of A on (L_1, L_N) using that basis. Similarly let ω_1', ω_2' be another basis for (L_1, L_N), and let α' be the action of A using that basis. Now we compute the matrix A' for α' in terms of the basis ω_1, ω_2. We find that $A' = T^{-1}AT$, where T is the transformation matrix taking the basis ω_1, ω_2 to the basis ω_1', ω_2'. Since both are bases for the same lattice pair, we have $T \in \Gamma_0(N)$.

Now we want to require that α and α' have the same effect when applied to (L_1, L_N). We notice that

$$\begin{aligned} \alpha(L_1, L_N) = \alpha'(L_1, L_N) &\Leftrightarrow A \equiv A' \qquad (\mathrm{mod}\ \Gamma_0(N)) \\ &\Leftrightarrow T^{-1}ATA^{-1} \in \Gamma_0(N) \\ &\Leftrightarrow ATA^{-1} \in \Gamma_0(N). \end{aligned}$$

The above computation was done for a specific ω_1', ω_2'. Now we find that when we let ω_1', ω_2' range over all possible bases of (L_1, L_N), then T ranges over all elements of $\Gamma_0(N)$. So the above equation holds for every basis of (L_1, L_N) exactly when ATA^{-1} is in $\Gamma_0(N)$ for all $T \in \Gamma_0(N)$, that is, exactly when A normalizes $\Gamma_0(N)$. ∎

One type of substitution we shall be using frequently is the Atkin–Lehner involution W_e. This is always in the normalizer of $\Gamma_0(N)$; so the preceding theorem applies, and the reader may verify that:

PROPOSITION 2.19. *Given a matrix W_e and a lattice pair (L_1, L_N),*

$$W_e(L_1, L_N) = \left(L_e, eL_{N/e}\right).$$

Furthermore, if $k \mid N$ *and* $L_k = \mathrm{Ind}_k(L_1, L_N)$, *let* $k = lm$, *where* $(l, e) = 1$ *and* $m \mid e$. *Then*

$$W_e L_k = mL_{le/m}.$$

2.5. *Fourier Series of Hauptmoduls*

We state here a few lemmas about Fourier series, which we shall use later in computing poles.

LEMMA 2.20. *If* $f(z) = \sum_{k=k_0}^{\infty} a_k q^k$, *then*

$$f\left(\frac{az + b}{d}\right) = \sum_{k=k_0}^{\infty} \zeta^k a_k q^{ak/d},$$

where ζ *is the root of unity* $e^{2\pi ib/d}$.

(The reader can easily verify this.)

LEMMA 2.21. *Let* f *be a Hauptmodul for some modular group* G, *and let* α *normalize* G. *Then*

$$f(\alpha z) = \frac{Af(z) + B}{Cf(z) + D}$$

for some $A, B, C, D \in \mathbf{C}$.

Proof. Since f is a Hauptmodul for G, we have the equivalence

$$f(z) = f(w) \Leftrightarrow z = \gamma w \qquad \text{for some } \gamma \in G.$$

Then we must also have the equivalences

$$\begin{aligned} f(\alpha z) = f(\alpha w) &\Leftrightarrow \alpha z = \gamma \alpha w \qquad \text{for some } \gamma \in G \\ &\Leftrightarrow \alpha z = \alpha \gamma' w \qquad \text{for some } \gamma' \in G \\ &\Leftrightarrow z = \gamma' w. \end{aligned}$$

So $f(\alpha z)$ is invariant under G, and therefore it is a rational function of $f(z)$. But $f(\alpha z)$ has only one zero and one pole (modulo G), so it must take the form shown. ∎

If $\alpha\infty \not\equiv \infty \pmod{G}$, this shows that there is no pole of $f(\alpha z)$ at $z = \infty$. In fact:

COROLLARY 2.22. *With* f, G, α *as above, let* $g(z) = P_m(f(z))$. *Then, if* $\alpha\infty \not\equiv \infty \pmod{G}$, $g(\alpha z)$ *has no pole at* $z = \infty$; *that is,* $g(\alpha z)$ *has leading term* 0.

2.6. *Locating Poles and Cusps*

We can now address the problem which arose a few sections ago when we tried to prove the replication formulae for J_{N-}. We want to compare the poles of $(mf \mid \hat{T}_m)(z)$ with the cusps of the fundamental region for $\Gamma_0(N)$, to see whether they coincide.

We begin by quoting the following two lemmas from [Fer1]:

LEMMA 2.23. *The images of ∞ on the real line under $\Gamma_0(N)$ are*

$$\left\{ \frac{a}{cN} \middle| (a, cN) = 1; a, c \in \mathbf{Z}; c \neq 0 \right\}.$$

LEMMA 2.24. *A fundamental region for $\Gamma_0(N)$ can be chosen so that its cusps on the real line are*

$$\left\{ \frac{k}{N} \middle| (k, N) > 1, \frac{-N}{2} \leq k \leq \frac{N}{2} \right\}.$$

LEMMA 2.25. *Suppose $f = P_m(J_{N-})$. Then*:

1. *If $p \nmid N$, none of the summands of $f \mid \hat{T}_p$ have poles at any real cusp of $\Gamma_0(N)$.*

2. *If $p \mid N$, none of the summands of $f \mid \hat{T}_p$ have poles at any real cusp of $\Gamma_0(N)$, except possibly at the cusps of the form k/N, where $(k, N) = p$.*

Proof. First suppose $p \nmid N$. The only poles of f are at ∞ and its images under $\Gamma_0(N)$, so by Lemma 2.23 we have

$$\{\text{poles of } f(pz)\} = \left\{ \frac{a}{cNp} \middle| (a, cN) = 1; a, c \in \mathbf{Z}; c \neq 0 \right\}$$

$$\left\{ \text{poles of } f\left(\frac{z + j}{p} \right) \right\} = \left\{ \frac{ap + jcN}{cN} \middle| (a, cN) = 1; a, c \in \mathbf{Z}; c \neq 0 \right\}.$$

Now we wonder whether any of these poles can take the form k/N for some k with $(k, N) > 1$. Since an N is present in all of the denominators already, it suffices to show that the numerators are all relatively prime to N. First we observe that $(a, N) = 1$, which rules out the poles of $f(pz)$; and $(ap + jcN, N) = (ap, N) = 1$, which rules out the poles of $f((z + j)/p)$. This proves case 1.

Next suppose $p \mid N$. The poles of $f((z + j)/p)$ are as before. But now $f^{(p)}$ has invariance group $\Gamma_0(N/p)$, so we have

$$\{\text{poles of } f^{(p)}(pz)\} = \left\{ \frac{a}{cN} \middle| (a, c(N/p)) = 1; a, c \in \mathbf{Z}; c \neq 0 \right\}.$$

We check the numerators as before. For the poles of $f^{(p)}(pz)$, we find $(a, N) = (a, p)$; and for the poles of $f((z + j)/p)$, we find $(ap + jcN, N) = (ap, N) = p$. Since in either case the only possible common factor is p, this proves case 2. ∎

So the only cases we need to check are those with $p \mid N$, at cusps of the form k/N where $(k, N) = p$. In these cases, several of the summands of $pf \mid \hat{T}_p$ will have poles there, and we shall show that the residues cancel.

THEOREM 2.26. *Let $f(z) = P_m(J_{N-})$, and let $p \parallel N$. Let m be any element of $\Gamma_0(N/p)$ not in $\Gamma_0(N)$. Then*

$$\left(pf \mid \hat{T}_p\right)(Mz) \text{ has leading term } \begin{cases} 0 & \text{if } p \nmid m \\ pq^{-m/p} & \text{if } p \mid m. \end{cases}$$

Proof. Let μ be the action of M on the basis $z, 1$. Let $L_k = \langle kz, 1\rangle$ and $L'_k = \mu L_k$ for all $k \mid N$. Then

$$\begin{aligned} pF \mid \hat{T}_p \mu(L_1, L_N) &= pF \mid \hat{T}_p(L_1, L'_N) \\ &= \sum_{[L_1 : L''] = p} F(L'', L'' \cap L'_N) \\ &= F(L'_p, L'_N) + F(L_p, pL_{N/p}) + \sum_{\substack{[L_1 : L''] = p \\ L'' \neq L'_p, L_p}} F(L'', pL_{N/p}) \\ &= F(L'_p, L'_N) + FW_p(L_1, L_N) + \sum_{\substack{[L_1 : L''] = p \\ L'' \neq L'_p, L_p}} F(L'', pL_{N/p}), \end{aligned}$$

noting that, by the definition of M, we have $L'_N \neq L_N$ but $L'_{N/p} = L_{N/p}$. Together these imply $L'_p \neq L_p$. Also, we note that, for any $L'' \neq L'_p$, we have

$$L'' \cap L'_N = L'' \cap L'_p \cap L'_{N/p} = pL \cap L'_{N/p} = pL'_{N/p}.$$

Now the sublattices of index p in L_1 are

$$\langle z, p\rangle; \langle z + 1, p\rangle; \ldots, \langle z + (p - 1), p\rangle; \qquad \text{and} \qquad \langle pz, 1\rangle = L_p.$$

So $L'_p = \langle z + k, p\rangle$ for some k, and the above formula becomes

$$\left(pf \mid \hat{T}_p\right)(Mz) = f^{(p)}\left(\frac{z + k}{p}\right) + f\left(W_p(z)\right) + \sum_{\substack{0 \le j < p \\ j \neq k}} f\left(\frac{z + j}{p}\right);$$

and, evaluating leading terms of Fourier series using Lemma 2.20 and Corollary 2.22, we find

$$\zeta^{km}q^{-m/p} + 0 + \sum_{\substack{0\le j<p\\ j\neq k}} \zeta^{jm}q^{-m/p} = \begin{cases} 0 & \text{if } p \nmid m \\ pq^{-m/p} & \text{if } p \mid m, \end{cases}$$

where $\zeta = e^{2\pi i/p}$. ∎

THEOREM 2.27. *Let $f(z) = P_m(J_{N-}(z))$. Let p be a prime such that $p^2 \mid N$. Let M be any element of $\Gamma_0(N/p)$. Then*

$$\left(pf \mid \hat{T}_p\right)(Mz) \text{ has leading term } \begin{cases} 0 & \text{if } p \nmid m \\ pq^{-m/p} & \text{if } p \mid m. \end{cases}$$

Proof. Since $p \mid N$, $f^{(p)}$ has invariance group $\Gamma_0(N/p)$. Applying Lemma 2.23 we have

$$\{\text{poles of } f^{(p)}(pz)\} = \left\{ \frac{a}{cN} \middle| (a, c(N/p)) = 1, a, c \in \mathbf{Z}, c \neq 0 \right\}.$$

Since $p \mid N/p$, the conditions $(a, c(N/p)) = 1$ and $(a, cN) = 1$ are equivalent. So none of these poles can satisfy $(a, N) > 1$, and none of them can exist at a cusp of $f(z)$. So we may restrict our attention to $pf \mid T_p$.

But by Corollary 3.10 in the next section we have

$$\begin{aligned} \left(pf \mid T_p\right)(Mz) &= \left(pf \mid T_p\right)(z) \\ &= f\left(\frac{z}{p}\right) + f\left(\frac{z+1}{p}\right) + \cdots + f\left(\frac{z+(p-1)}{p}\right), \end{aligned}$$

and on evaluating Fourier series, we find the sum either has no pole (if $p \nmid m$), or has leading term $pq^{-m/p}$ (if $p \mid m$), as claimed. ∎

2.7. *Replication for* $\Gamma_0(N)$

Now that we have resolved the problem of finding poles and cusps, we can proceed to prove the replication formulae for Hauptmoduls J_{N-}.

THEOREM 2.28. *Every Hauptmodul J_{N-} is completely replicable, with replicates as given by the power-map rule.*

Proof. We want to show that $mf \mid \hat{T}_m = P_m(f)$ for any $f = J_{N-}$ and for any m. We proceed by double induction, first on N and then on m. In the

base cases, we observe that $N = 1$ has already been done as Proposition 2.17, while $m = 1$ is trivial since $f \mid \hat{T}_1 = P_1(f) = f$.

In the general case, we may assume the statement holds for all $N' < N$, and for all $m' < m$ for the current N. By Proposition 2.14, $mf \mid \hat{T}_m$ has invariance group $\Gamma_0(N)$, and its Fourier series has leading term q^{-m}. So the only difficulty is to show that $mf \mid \hat{T}_m$ has no poles (modulo $\Gamma_0(N)$) except at ∞. Since $m > 1$, we may pick a prime p such that $p \mid m$, and let $l = m/p$. Then, by Corollary 2.7 and the induction hypotheses,

$$mf \mid \hat{T}_m = \begin{cases} mf \mid \hat{T}_l \hat{T}_p & = pP_l(f) \mid \hat{T}_p \quad \text{if } p \parallel m \\ mf \mid \hat{T}_l \hat{T}_p - mpf \mid \hat{R}_p \hat{T}_{l/p} & = pP_l(f) \mid \hat{T}_p - pP_{l/p}(f^{(p)}) \quad \text{if } p^2 \mid m. \end{cases}$$

Now there are four cases.

1. If $p \nmid N$ and $p \parallel m$, then $pP_l(f) \mid \hat{T}_p$ has no poles at any real cusp of $\Gamma_0(N)$ by Lemma 2.25.

2. If $p \nmid N$ and $p^2 \mid m$, then $pP_l(f) \mid \hat{T}_p - pP_{l/p}(f^{(p)})$ has no poles at any real cusp of $\Gamma_0(N)$: we handle $pP_l(f) \mid \hat{T}_p$ as in case 1, and we observe directly that $pP_{l/p}(f^{(p)})$ has no such poles since $f^{(p)} = f = J_{N-}$.

3. If $p \mid N$ and $p \parallel m$, then by Lemma 2.25 we need only check the cusps of the form k/N, where $(k, N) = p$. For any such cusp, there exist a, b such that $ak + bN = p$. Then the matrix

$$M = \begin{pmatrix} a & b \\ -N/p & k/p \end{pmatrix}$$

maps k/N to ∞, and $M \in \Gamma_0(N/p) - \Gamma_0(N)$. We can then use either Lemma 2.26 or Lemma 2.27, together with the fact that $p \nmid l$, to conclude that $mf \mid \hat{T}_m$ has no poles at that cusp.

4. If $p \mid N$ and $p^2 \mid m$, then as in case 3, the only cusps that need checking are of the form k/N with $(k, N) = p$. These can be moved to ∞ by some $M \in \Gamma_0(N/p) - \Gamma_0(N)$. Again we refer to either Lemma 2.26 or Lemma 2.27, this time with $p \mid l$, to find that $(pP_l(f) \mid \hat{T}_p)(Mz)$ has leading term $pq^{-l/p}$. Now since M is in $\Gamma_0(N/p)$, which is the invariance group of $f^{(p)}$, we have $f^{(p)}(Mz) = f^{(p)}(z)$, so $pP_{l/p}(f^{(p)}(Mz))$ has leading term $pq^{-l/p}$. These two quantities cancel, so the sum $(mf \mid \hat{T}_m)(Mz)$ has no poles at that cusp. ∎

3. REPLICATION ON $n|h$-TYPE GROUPS

In the preceding section, we proved replication for functions whose invariance groups were *exactly* $\Gamma_0(N)$. We now extend these methods to deal with larger groups, which contain normalizer elements of $\Gamma_0(N)$. Many of these proofs are similar to (though more tedious than) those of the preceding section, so some details will be omitted.

3.1. *Hecke Operators and Normalizer Elements*

Consider the Hauptmodul $f = J_{n|h+e_1,e_2,\ldots}$ of the general $n|h$-type group $(1/h)\Gamma_0(n|h) + e_1, e_2, \ldots$. For such a group we define $N = nh$. As before we can identify f with a function F on lattice pairs (L_1, L_N): by definition f is invariant under $\Gamma_0(N)$, and we can verify that its replicates are invariant under the appropriate groups:

PROPOSITION 3.1. *Suppose* $f = J_{n|h+e_1,e_2,\ldots}$ (*or* $P_m(J_{n|h+e_1,e_2,\ldots})$), *with replicates defined by the power-map rule. Then its replicates satisfy Proposition* 2.8.

Proof. We begin by noting that $f^{(a)}$ is of type $n'|h' + e_1', e_2', \ldots$, with $n' = n/(a,n)$ and $h' = h/(a,h)$. Define $N' = N/(a,N)$. We see that $(a,nh)|(a,n)(a,h)$, so that

$$n'h' = \frac{n}{(a,n)} \cdot \frac{h}{(a,h)} \Bigg| \frac{nh}{(a,nh)} = \frac{N}{(a,N)} = N'.$$

So $\Gamma_0(N')$ is contained in $\Gamma_0(n'h')$, which is in the fixing group of $f^{(a)}$.

If $a|N$, we have $N' = N/a$, and this proves property 1. If $a \nmid N$, we can replace a by (a,N); this will leave N', n', h', and the e_i''s unchanged, which proves property 2. ∎

So Proposition 2.14 applies to f, and $f|\hat{T}_m$ is invariant under $\Gamma_0(N)$.

We now wish to show that $f|\hat{T}_m$ has a larger invariance group, namely, the same invariance group as f. To do this we investigate how lattice pairs interact with normalizer elements. First we prove the following general lemma:

LEMMA 3.2. *Let* α *be any lattice isomorphism* $\alpha\colon L_1 \to \bar{L}$, *and let* L' *and* L_N *be sublattices of* L_1. *Then*

$$a\hat{T}_m(L_1, L_N) = \hat{T}_m(\alpha L_1, \alpha L_N)$$
$$\alpha T_m(L_1, L_N) = T_m(\alpha L_1, \alpha L_N).$$

Proof. First we note that

$$\alpha \hat{T}_m(L_1, L_N) = \frac{1}{m} \sum_{[L_1 : L'] = m} \alpha(L', L' \cap L_N)$$

$$= \frac{1}{m} \sum_{[L_1 : L'] = m} (\alpha L', \alpha L' \cap \alpha L_N)$$

$$\hat{T}_m \alpha(L_1, L_N) = \hat{T}_m(\alpha L_1, \alpha L_N)$$

$$= \frac{1}{m} \sum_{[\alpha L_1 : L''] = m} (L'', L'' \cap \alpha L_N).$$

Now each $\alpha L'$ is a sublattice of index m in αL, and so must be one of the L''. And conversely, each L'' must be an $\alpha L'$ for some L'; so the two sums are equal. This proves the first equation. The second is proved in the same manner, with the extra condition $L'/(L' \cap L_N) \cong C_N$ placed on the first sum, and similar conditions placed on the other sums. ∎

We can now apply the above lemma to the specific cases of normalizer elements.

THEOREM 3.3. *Let (L_1, L_N) be a lattice pair of type N, and $A = \left(\begin{smallmatrix} a & b/h \\ cn & d \end{smallmatrix}\right)$ an element of $\Gamma_0(n \mid h)$. If p is a prime such that $p \mid c$ and $p \nmid h$, then*

$$T_p A(L_1, L_N) = A' T_p(L_1, L_N)$$

$$\hat{T}_p A(L_1, L_N) = A' \hat{T}_p(L_1, L_N)$$

where $A' = \left(\begin{smallmatrix} a & bp/h \\ cn/p & d \end{smallmatrix}\right)$.

Proof. Let ω_1, ω_2 be a basis for (L_1, L_N), and let α be the isomorphism of L whose action with respect to ω_1, ω_2 is given by the matrix A. Then, by Lemma 3.2,

$$T_p \alpha(L_1, L_N) = \alpha T_p(L_1, L_N)$$

$$\hat{T}_p \alpha(L_1, L_N) = \alpha \hat{T}_p(L_1, L_N).$$

So now we need to find a matrix which expresses the action of α on a sublattice L' of index p in L_1. For the moment, we will assume that if $p \mid N$ then $L' \neq L_p$. By the structure theorem we may pick a new basis ω_1', ω_2' for (L_1, L_N) such that $L' = \langle \omega_1', p\omega_2' \rangle$. Since A normalizes $\Gamma_0(N)$

we may assume that A expresses the action of α with respect to ω_1', ω_2'. Then the matrix of α with respect to $\omega_1', p\omega_2'$ is

$$\begin{pmatrix} 1 & 0 \\ 0 & 1/p \end{pmatrix}\begin{pmatrix} a & b/h \\ cn & d \end{pmatrix}\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} = \begin{pmatrix} a & bp/h \\ cn/p & d \end{pmatrix},$$

which is how we defined A' above.

We now consider the special case when $p \mid N$ and $L' = L_p$. In this case we know that $L' = \langle p\omega_1, \omega_2 \rangle$, and that the matrix of α with respect to $p\omega_1, \omega_2$ is

$$\begin{pmatrix} 1/p & 0 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} a & b/h \\ cn & d \end{pmatrix}\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b/hp \\ cnp & d \end{pmatrix}.$$

(Note that, by Lemma 1.3, we may assume without loss of generality that $p \mid b$.) But we now observe that, since $p \nmid h$ and $h \mid 24$, we have $p^2 \equiv 1 \pmod{h}$. This implies that $b/p \equiv bp \pmod{h}$ and $cp \equiv c/p \pmod{h}$, so that this matrix is equivalent modulo $\Gamma_0(N)$ to A', and thus A' can equally well be used to give the action of α with respect to $p\omega_1, \omega_2$.

It remains to show that A' can be substituted for α. Since $A' \in \Gamma_0(n \mid h)$, we know that A' normalizes $\Gamma_0(N)$; and since all lattice pairs in $T_p(L_1, L_N)$ are of type N, the substitution is valid in the T_p case. In the $\hat{T}_p$ case, there may also be a lattice pair of type N/p. If this is so, $p \mid N$, and since $p \nmid h$ we have $p \mid n$. Now since $A' \in \Gamma_0(n \mid h) \subset \Gamma_0((n/p) \mid h)$, it normalizes $\Gamma_0(nh/p) = \Gamma_0(N/p)$. So we can still substitute A' for α, and the proof is done. ∎

When A is an element of the fixing group $F_1(f)$, we know by Theorem 1.4 that $A' \in F_1(f)$ as well. So we have:

COROLLARY 3.4. *If $f = P_m(J_{n \mid h+e_1, e_2, \ldots})$, and if $p \nmid h$, then $f \mid \hat{T}_p$ is invariant under $F_1(f)$.*

THEOREM 3.5. *Let (L_1, L_N) be a lattice pair of type N, and let $E \parallel N$ and $p \nmid E$. Then*

$$W_E T_p(L_1, L_N) = T_p W_E(L_1, L_N)$$

$$W_E \hat{T}_p(L_1, L_N) = \hat{T}_p W_E(L_1, L_N).$$

Proof. Let $A = \left(\begin{smallmatrix} aE & b \\ cN & dE \end{smallmatrix}\right)$ be a W_E matrix for $\Gamma_0(N)$. Without loss of generality we may assume $p \mid b$ and $p \mid c$ (pick a W_E matrix for $\Gamma_0(p^2N)$ and conjugate it by $\left(\begin{smallmatrix} 1 & 0 \\ 0 & p \end{smallmatrix}\right)$). Let ω_1, ω_2 be a basis for (L_1, L_N). Let α be the mapping obtained by the action of A on the basis ω_1, ω_2. Then by Lemma

3.2 we have

$$\alpha T_p(L_1, L_N) = T_p \alpha(L_1, L_N)$$
$$\alpha \hat{T}_p(L_1, L_N) = \hat{T}_p \alpha(L_1, L_N).$$

Now the matrix for α on a sublattice of index p is either $\left(\begin{smallmatrix} aE & bp \\ cN/p & dE \end{smallmatrix}\right)$ or $\left(\begin{smallmatrix} aE & b/p \\ cpN & dE \end{smallmatrix}\right)$, by a conjugation argument similar to that of Theorem 3.3. Either of these is a W_E matrix for $\Gamma_0(N)$. We also note that (L_1, L_N) is a lattice pair of type N, as are all of the summands in $T_p(L_1, L_N)$ by definition of T_p. So in the first equation we can replace every α by W_E unambiguously, by Theorem 2.18.

For the second equation we use the additional assumption that $p \nmid E$. Every summand in $\hat{T}_p(L_1, L_N)$ is either of type N or type N/p. Since $p \nmid E$, we must have $E \| (N/p)$. It then follows that W_E normalizes $\Gamma_0(N/p)$, and again we can replace every α by W_E. ∎

Applying this to functions, it clearly follows that:

COROLLARY 3.6. *If $f = P_m(J_{n \mid h+e_1, e_2, \ldots})$, and if p is a prime such that $p \nmid h$ and $p \nmid e_i$, then $f \mid \hat{T}_p$ is invariant under W_{e_i}.*

3.2. *Compression Formulae*

Equation 1 of the following theorem was observed in [CoN] and called the "compression formula"; several variants, including Eqs. 2 and 3, were proved in [Koi].

THEOREM 3.7 (Compression Formulae). *Let $f = J_{np \mid h+e_1, e_2, \ldots}$, where $p \nmid h$. Then*:

1. *If p is one of the e_i, then*

$$f^{(p)}(z) = f(z) + f\left(\frac{z}{p}\right) + f\left(\frac{z+1}{p}\right) + \cdots + f\left(\frac{z+(p-1)}{p}\right).$$

2. *If p is not one of the e_i, but ep is, for some e with $p \nmid e$, then*

$$f^{(p)}(W_e z) = f(W_p z) + f\left(\frac{z}{p}\right) + f\left(\frac{z+1}{p}\right) + \cdots + f\left(\frac{z+(p-1)}{p}\right).$$

3. *If ep is one of the e_i, for some e with $p \mid e$, then*

$$f^{(p)}(W_e z) = f\left(\frac{z}{p}\right) + f\left(\frac{z+1}{p}\right) + \cdots + f\left(\frac{z+(p-1)}{p}\right).$$

To prove these we first define a new operator:

DEFINITION 3.8. For any prime p, we define the *compression operator* $\hat{C}_p$ by the formula

$$\hat{C}_p(L_1, L_N) = \frac{1}{p} \sum_{\substack{[L_1 : L'] = p \\ L'/pL_N \cong C_{pN}}} (L', pL_N).$$

THEOREM 3.9. *For any lattice pair* (L_1, L_{pN}) *let* $L_N = \mathrm{Ind}_N(L_1, L_{pN})$. *Then*

$$p\hat{C}_p(L_1, L_N) = \begin{cases} pT_p(L_1, L_{pN}) + W_p(L_1, L_{pN}) & \text{if } p \nmid N \\ pT_p(L_1, L_{pN}) & \text{if } p \mid N. \end{cases}$$

Proof. Let $L_p = \mathrm{Ind}_p(L_1, L_{pN})$. In the $p \nmid N$ case we have

$$\begin{aligned} p\hat{C}_p(L_1, L_N) &= \sum_{\substack{[L_1 : L'] = p \\ L'_1 \neq L_p}} (L', pL_N) + (L_p, pL_N) \\ &= \sum_{\substack{[L_1 : L'] = p \\ L'_1 \neq L_p}} (L', L_{pN} \cap L') + (L_p, pL_N) \\ &= pT_p(L_1, L_{pN}) + W_p(L_1, L_{pN}). \end{aligned}$$

The $p \mid N$ case is similar, except that L_p/pL_N is isomorphic to $C_p \times C_N$, which is not isomorphic to C_{pN}. So the last term on the right-hand side is omitted throughout. ∎

COROLLARY 3.10. *Let* (L_1, L_N) *be a lattice pair of type* N, *and let* μ *be a mapping which fixes* L_1 *and* $L_{N/p} = \mathrm{Ind}_{N/p}(L_1, L_N)$, *where* p *is prime and* $p^2 \mid N$. *Then*

$$T_p \mu(L_1, L_N) = T_p(L_1, L_N).$$

Proof. By Theorem 3.9 both are equal to $\hat{C}_p(L_1, L_{N/p})$. ∎

COROLLARY 3.11. *Let* (L_1, L_N) *be a lattice pair, and let* p *be prime. Then*:

1. *If* $p \nmid e$,

$$\hat{C}_p W_e(L_1, L_N) = W_e \hat{C}_p(L_1, L_N).$$

2. *If* $A = \left(\begin{smallmatrix} a & b/h \\ cn & d \end{smallmatrix}\right)$ *is an element of* $\Gamma_0(n \mid h)$ *such that* $p \mid c$ *and* $p \nmid h$,

then

$$\hat{C}_p A(L_1, L_N) = A' \hat{C}_p(L_1, L_N),$$

where $A' = \left(\begin{smallmatrix} a & bp/h \\ cn/p & d \end{smallmatrix}\right)$.

Proof. We use the expressions for $\hat{C}_p$ given by Theorem 3.9. To prove statement 1, we note that W_e is known to commute with both T_p (by Theorem 3.5) and W_p (by Theorem 2.7 of [Fer1]). Similarly, statement 2 is proved by combining Theorem 3.3 with Lemma 2.6 from [Fer1]. ∎

Proof of Compression Formulae. We prove formula 1 only; the others are proved similarly. Let F be the function on lattice pairs corresponding to the function f on $\mathbf{H}^+$, and let G be the composition of F and $\hat{C}_p$. Then, by Theorem 3.9, we have

$$pG(L_1, L_N) = pF\big(T_p(L_1, L_{pN})\big) + F\big(W_p(L_1, L_{pN})\big),$$

or equivalently,

$$g(z) = f\left(\frac{z}{p}\right) + f\left(\frac{z+1}{p}\right) + \cdots + f\left(\frac{z+(p-1)}{p}\right) + f(W_p z),$$

where the function g corresponding to G is invariant under $\Gamma_0(N)$.

By Corollary 3.11, if $p \nmid e_i$ and f is invariant under W_{e_i}, so is g. Also, by Corollaries 1.5 and 3.11, g must be invariant under $F_1(f^{(p)})$, so we see that g has the full invariance group of $f^{(p)}$.

Now we know that $f(W_p z) = f(z)$. So all that remains is to show that $g = f^{(p)}$, and we do this by examining the poles of $g(z)$ in the sum above. By adding the Fourier series of the f's we see that g has a Fourier series with leading term q^{-1}, so we need only show that it has no poles elsewhere. Since f is holomorphic on $\mathbf{H}^+$ it suffices to check the real line.

We quote the following results from [Fer1]:

LEMMA 3.12. *The fundamental region for* $(1/h)\Gamma_0(n \mid h) + e_1, e_2, \ldots$ *can be chosen such that its cusps on the real line are contained in the set*

$$\left\{ \frac{k}{n} \,\middle|\, \left(k, \frac{n}{h}\right) \neq e_i \ \forall i, \frac{-n}{2} \leq k \leq \frac{n}{2} \right\}.$$

LEMMA 3.13. *The images of* ∞ *on the real line under* $(1/h)\Gamma_0(n \mid h) + e_1, e_2, \ldots$ *are*

$$\bigcup_e \left\{ \frac{ae}{cn} \,\middle|\, \left(ae, c\frac{n}{h}\right) = e; a, c \in \mathbf{Z}; c \neq 0 \right\}.$$

Let $\{1, e_1', e_2', \dots\}$ be the set of e_i's under which $f^{(p)}$ is invariant. Then every e_i is either an e_i' or equal to $e_i' p$ for some i. With this notation we list the poles of the f's:

$$\{\text{poles of } f(z)\} = \bigcup_{e'} \left\{ \frac{ae'}{cnp} \middle| \left(ae'^2, c\frac{np}{h} \right) = e' \right\} \cup \bigcup_{e'} \left\{ \frac{ae'p}{cnp} \middle| \left(a(e'p)^2, c\frac{np}{h} \right) = e'p \right\}$$

$$\left\{ \text{poles of } f\left(\frac{z+j}{p} \right) \right\} = \bigcup_{e'} \left\{ \frac{ae' + jcn}{cn} \middle| \left(ae'^2, c\frac{np}{h} \right) = e' \right\} \cup \bigcup_{e'} \left\{ \frac{ae'p + jcn}{cn} \middle| \left(a(e'p)^2, c\frac{np}{h} \right) = e'p \right\}.$$

Now the fundamental region for $(1/h)\Gamma_0(n \mid h) + e_1', e_2', \dots$ has cusps on the real line at the points $\{(k/n) \mid (k, n/h) \neq e_i', \forall i\}$. We check the four sets of poles to see whether they coincide with these. In the first set, since $p \nmid e'$, the p in the denominator can never cancel; in the second set, the p does cancel, but it leaves a numerator whose gcd with n is an e'. And in the last two sets the gcd of the numerator with n must be an e'. So none of these poles occur at cusps of $g(z)$, and we are done. ∎

In the above proof, we assumed that f is a Hauptmodul. However, the same proof can easily be generalized to deal with other functions in the following manner:

COROLLARY 3.14. *With f as above, let* $g = P_m(J_{n \mid h + e_1, e_2, \dots})$. *Then*:

1. *If* $p \nmid m$, *the appropriate compression formula still holds for g.*

2. *If* $p \mid m$, *the appropriate compression formula holds for g if the extra term* $pP_{m/p}(f^{(p)})$ *is added to the left-hand side.*

Proof. As above, except that certain sums of Fourier series give an extra term in the $p \mid m$ case. ∎

3.3. *Expanding the Invariance Group*

We now use the results of the preceding two sections to show that certain values of $f \mid \hat{T}_p$ have the appropriate invariance group.

THEOREM 3.15. *Let* $f = P_m(J_{n \mid h + e_1, e_2, \dots})$, *and let e be one of the* e_i*'s. Let p be a prime such that* $p \nmid h$ *and* $p \mid e$. *Then*:

1. *If* $p \nmid m$, *then* $pf \mid \hat{T}_p$ *is invariant under* W_e.

2. *If $p \mid m$, then the quantity $pf \mid \hat{T}_p - pP_{m/p}(J^{(p)}_{n \mid h+e_1, e_2, \dots})$ is invariant under W_e.*

Proof. We prove the first statement only; the proof of the second is similar. We distinguish two cases:

1. If $p \parallel e$, let $\epsilon = e/p$. Then we have

$$\begin{aligned}\left(pf \mid \hat{T}_p\right)(z) &= f^{(p)}(pz) + \sum_{j=0}^{p-1} f\left(\frac{z+j}{p}\right) \\ &= f^{(p)}(pz) + f^{(p)}(W_\epsilon z) - f(W_\epsilon z),\end{aligned}$$

where this substitution comes from either the first compression formula (if W_p is present), or from the second (otherwise). The last term in this equation is clearly invariant under $W_{\epsilon p}$, since $W_{\epsilon p}$ commutes with W_ϵ. So we need to show that the sum of the first two terms is invariant as well.

We rewrite the above equation in lattice form. Let $L_1 = \langle z, 1\rangle$ and $L_{pN} = \langle pNz, 1\rangle$, and for $k \mid N$ define $L_k = \mathrm{Ind}_k(L_1, L_N)$ as usual. Then the first two terms of the above equation become

$$F(L_p, L_{pN}) + FW_\epsilon(L_1, L_N) = F(L_p, L_{pN}) + F(L_\epsilon, \epsilon L_{N/\epsilon}).$$

Now $W_{\epsilon p}(L_1, L_{pN}) = (L_{\epsilon p}, \epsilon p L_{N/\epsilon})$, so replacing F by $FW_{\epsilon p}$ gives

$$F(pL_\epsilon, \epsilon p L_{N/\epsilon}) + F(\epsilon L_p, \epsilon L_{pN}),$$

which is equal to the preceding quantity, by the scalar multiplication property of F. So we are done.

2. If $p^2 \mid e$, let $\epsilon = e/p$ as before. Then

$$\begin{aligned}\left(pf \mid \hat{T}_p\right)(z) &= f^{(p)}(pz) + \sum_{k=0}^{p-1} f\left(\frac{z+k}{p}\right) \\ &= f^{(p)}(pz) + f^{(p)}(W_\epsilon z),\end{aligned}$$

this time using the third compression formula. This quantity is shown to be invariant under $W_{\epsilon p}$, using the same proof as above. ∎

THEOREM 3.16. *Let $f = P_m(J_{n \mid h+e_1, e_2, \dots})$, and let p be a prime not dividing h.*

1. *If $p \nmid m$, then $f \mid \hat{T}_p$ is invariant under $F(f)$.*

2. *If $p \mid m$, then the quantity $pf \mid \hat{T}_p - pP_{m/p}(J^{(p)}_{n \mid h+e_1, e_2, \dots})$ is invariant under $F(f)$.*

Proof. We first note that $f \mid \hat{T}_p$ is invariant under $\Gamma_0(N)$ by Proposition 2.14. Next, we observe that

$$\frac{\Gamma_0(n \mid h) + e_1, e_2, \dots}{\Gamma_0(N)} = \frac{\Gamma_0(n \mid h)}{\Gamma_0(N)} \cdot \langle W_{E_1}, W_{E_2}, \dots \rangle,$$

so it suffices to show invariance under two types of normalizer elements:

1. elements of $F_1(f) = F(f) \cap \Gamma_0(n \mid h)$, which are covered by Corollary 3.4; and

2. Atkin–Lehner involutions W_E, which are covered by Corollary 3.6 if $p \nmid E$, or by Theorem 3.15 if $p \mid E$. ∎

3.4. *Poles and Cusps in the $n \mid h$ Case*

We now develop results regarding poles and cusps of $f \mid \hat{T}_p$ for general $n \mid h$-type Hauptmoduls f. The method is similar to that of Section 2.6.

LEMMA 3.17. *Suppose $f = P_m(J_{n \mid h + e_1, \dots})$.*

1. *If $p \nmid (n/h)$, none of the summands of $f \mid \hat{T}_p$ have poles at any real cusp of the group $(1/h)\Gamma_0(n \mid h) + e_1, e_2, \dots$.*

2. *If $p \mid (n/h)$, none of the summands of $f \mid \hat{T}_p$ have poles at any real cusp of the group $(1/h)\Gamma_0(n \mid h) + e_1, e_2, \dots$, except possibly at cusps of the form k/n with $(k, n/h) = p$ (and at cusps equivalent to these under W_e's).*

Proof. The proof is similar to that of Lemma 2.25, using the results of Lemma 3.13. The details are left to the reader. ∎

We next prove that in the $p \mid n$ cases from above, the poles still cancel. This is done by proving the analogues of Theorems 2.26 and 2.27 from the previous section. Recall that $F(f)$ is the fixing group of the function f, and $F_1(f)$ is its subgroup of elements of determinant 1.

THEOREM 3.18. *Let $f(z) = P_m(J_{n \mid h + e_1, e_2, \dots})(z)$, where w_p is not present, and let p be a prime with $p \| n$ and $p \nmid h$. Let M be any element of $F_1(f^{(p)}) - F_1(f)$. Then*

$$\left(pf \mid \hat{T}_p\right)(Mz) \text{ has leading term } \begin{cases} 0 & \text{if } p \nmid m \\ pq^{-m/p} & \text{if } p \mid m. \end{cases}$$

Proof. Suppose $M = \left(\begin{smallmatrix} a & b/h \\ c(n/p) & d \end{smallmatrix}\right)$. By Lemma 1.3 we may pick a', b', c', d' such that $p \mid c'$ and

$$\begin{pmatrix} a & b/h \\ c(n/p) & d \end{pmatrix} \equiv \begin{pmatrix} a' & b'/h \\ c'(n/p) & d' \end{pmatrix} \pmod{\Gamma_0(N/p)}.$$

This new matrix, which we shall call M', is in $F_1(f^{(p)})$, because M and M' are congruent modulo $\Gamma_0(N/p)$; and since $p \mid c'$, by Corollary 1.5 we see that M' is also in $F_1(f)$. So we can write $M = M'M_1$ with $M' \in F_1(f)$ and $M_1 \in \Gamma_0(N/p) - \Gamma_0(N)$. We also have, by Theorem 3.3,

$$f \mid \hat{T}_p M'M_1 = f \mid M''\hat{T}_p M_1 = f \mid \hat{T}_p M_1$$

where $M'' \in F_1(f)$. So it suffices to prove the theorem for $M \in \Gamma_0(N/p) - \Gamma_0(N)$.

The proof then proceeds as in Theorem 2.26. ∎

THEOREM 3.19. *Let $f(z) = P_m(J_{n \mid h+e_1, e_2, \ldots}(z))$. Let p be a prime such that $p^2 \mid n$ and $p \nmid h$. Let M be any element of $F_1(f^{(p)}) - F_1(f)$. Then*

$$\left(pf \mid \hat{T}_p\right)(Mz) \text{ has leading term } \begin{cases} 0 & \text{if } p \nmid m \\ pq^{-m/p} & \text{if } p \mid m. \end{cases}$$

Proof. First, we note that it suffices to consider $M \in \Gamma_0(N/p) - \Gamma_0(N)$, by the reasoning in Theorem 3.18.

Next we show that $f^{(p)}(p(Mz))$ has no pole at $z = \infty$. Applying Lemma 3.13 to $f^{(p)}$ we have

$$\text{poles of } f^{(p)}(pz) = \bigcup_e \left\{ \frac{ae}{cn} \,\middle|\, (ae^2, c(n/hp)) = e; a, c \in \mathbf{Z}; c \neq 0 \right\}.$$

Suppose $M^{-1}\infty$ was a pole of $f^{(p)}(pz)$. We know that $M^{-1}\infty$ has the form $a'/c'(N/p)$, where $(a', c'N/p) = 1$ and $p \nmid c'$ (otherwise M would be in $\Gamma_0(N)$). So to express this fraction in the form ae/cn, we must multiply both numerator and denominator by p. Then, since $p \mid (n/hp)$, we must have $p \mid (ae^2, c(n/hp))$. But $f^{(p)}$ is of type $(n/p) \mid h + e_1', e_2', \ldots$, where the e_i' are exact divisors of n/h which also divide n/ph. This implies that $p \nmid e$ for all e present in $f^{(p)}$, which contradicts our assumption that $(ae^2, c(n/hp)) = e$. So we conclude that $M^{-1}\infty$ is not among the poles of $f^{(p)}(pz)$, or equivalently, that ∞ is not among the poles of $f^{(p)}(p(Mz))$. So instead of looking at $pf \mid \hat{T}_p$ we may restrict our attention to $pf \mid T_p$.

The proof then proceeds as in Theorem 2.27. ∎

3.5. *The Polynomial Rule*

In their explicit constructions of the Monstrous Moonshine Hauptmoduls, Conway and Norton expressed the $n \mid h$-type Hauptmoduls with $h > 1$ as hth roots of their replicates. This happens in general, as we shall now prove; as a result, the values of $f \mid \hat{T}_p$ can be computed directly whenever $p \mid h$.

Throughout this section we will suppose that $f = J_{n \mid h+e_1, e_2, \ldots}$, and that p is a prime which divides h.

PROPOSITION 3.20. *Let k be any integer. Then $f(z + k/h) = \zeta^{-k} f(z)$, where $\zeta = e^{2\pi i/h}$.*

Proof. Since $\left(\begin{smallmatrix} 1 & k/h \\ 0 & 1 \end{smallmatrix}\right)$ normalizes the invariance group of f, by Lemma 2.21 we have

$$f\left(z + \frac{k}{h}\right) = \frac{Af(z) + B}{Cf(z) + D}$$

for some $A, B, C, D \in \mathbf{C}$. But the pole of $f(z + k/h)$ is at ∞, so C must equal 0. So D must be nonzero, and by rescaling we may assume $D = 1$. Then we note that the Fourier series of $f(z + k/h)$ has leading term $\zeta^{-k} q^{-1}$ and constant term 0. So we must have $A = \zeta^{-k}$ and $B = 0$. ∎

LEMMA 3.21. *$f(z) = (f^{(p)}(pz) + c)^{1/p}$ for some constant c.*

Proof. We define the function $g(z) = f(z/p)^p$. The invariance group of g obviously contains $H_p(F(f))$, where H_p denotes conjugation by $\left(\begin{smallmatrix} p & 0 \\ 0 & 1 \end{smallmatrix}\right)$ as in Lemma 1.6. Also, using Proposition 3.20 we can see that $g(z + 1) = g(z)$, so that g is invariant under the map $z \mapsto z + 1$. By Lemma 1.6, this proves that g is invariant under $F(f^{(p)})$.

Next we check for poles. We note that $f(z/p)$ has no poles modulo $H_p(F(f))$ except at ∞, by definition of f; therefore the same is true of $g(z)$. Also, if g has a pole at z_0, by Proposition 3.20 it also has one at $z_0 + 1$. Again by Lemma 1.6, this shows that g has no poles modulo $F(f^{(p)})$ except at ∞.

Finally, since g is invariant under $z \mapsto z + 1$, it has a Fourier series in terms of q, and using the Fourier series of f we find that

$$g(z) = q^{-1} + c + \text{positive powers of } q,$$

for some constant c. So g is, up to a constant, the Hauptmodul $f^{(p)}(z)$, and we have

$$f^{(p)}(z) = f\left(\frac{z}{p}\right)^p - c.$$

We now replace z by pz and solve for $f(z)$ to give the desired result. ∎

COROLLARY 3.22. *Suppose $p \mid m$. Then $(P_m(f))(z) = (P_{m/p}(f^{(p)}))(pz)$.*

Proof. First we suppose $m = p$. From the preceding lemma we know that

$$f(z)^p - c = f^{(p)}(pz).$$

The left-hand side of this equation is clearly a polynomial in $f(z)$, while the right-hand side, when expressed in terms of $q = e^{2\pi iz}$, has leading term q^{-p}. So this quantity is in fact $(P_p(f))(z)$, which proves the $m = p$ case.

In general, note that $(P_{m/p}(f^{(p)}))(pz)$ has leading term q^{-m}. This quantity must be a polynomial in $f(z)$, since we know from the $m = p$ case that $f^{(p)}(pz)$ is a polynomial in $f(z)$. So by definition it must equal $(P_m(f))(z)$. ∎

THEOREM 3.23. *Suppose $g = P_m(f)$. Then*

$$pg \mid T_p = \begin{cases} 0 & \text{if } p \nmid m \\ pP_{m/p}(f^{(p)}) & \text{if } p \mid m. \end{cases}$$

Proof. We observe that

$$\begin{aligned} \big(pg \mid T_p\big)(z) &= \sum_{0 \le k < p} g\left(\frac{z+k}{p}\right) \\ &= \sum_{0 \le k < p} \zeta^{km} g\left(\frac{z}{p}\right) = \begin{cases} 0 & \text{if } p \nmid m \\ pg(z/p) & \text{if } p \mid m. \end{cases} \end{aligned}$$

But in the $p \mid m$ case we know from Corollary 3.22 that

$$g(z) = \big(P_m(f)\big)(z) = \big(P_{m/p}(f^{(p)})\big)(pz),$$

and using this identity on the last line completes the proof. ∎

COROLLARY 3.24. *Suppose $g = P_m(f)$. Then*

$$pg \mid \hat{T}_p = \begin{cases} P_{mp}(f) & \text{if } p \nmid m \\ P_{mp}(f) + pP_{m/p}(f^{(p)}) & \text{if } p \mid m. \end{cases}$$

Proof. Add $(P_{mp}(f))(z)$ to the right side of Theorem 3.23, and $(P_m(f^{(p)}))(pz)$ to the left side. (By Corollary 3.22 these are equal.) ∎

3.6. *Replication for* $(1/h)\Gamma_0(n \mid h) + e_1, e_2, \ldots$

We have finally developed all of the tools needed to accomplish our major goal, that of proving the replicability of all $n \mid h$-type Hauptmoduls.

THEOREM 3.25. *Every $n \mid h$-type Hauptmodul $J_{n \mid h+e_1, e_2, \ldots}$ is completely replicable, with replicates as given by the power-map rule.*

Proof. We want to show that $mf \mid \hat{T}_m = P_m(f)$ for $f = J_{n \mid h+e_1, e_2, \dots}$ and for any m. We proceed by double induction on n and m as in Theorem 2.28. For $m > 1$, we may pick a prime p such that $p \mid m$, and let $l = m/p$. By Corollary 2.7 and the induction hypotheses,

$$mf \mid \hat{T}_m = \begin{cases} mf \mid \hat{T}_l \hat{T}_p & = pP_l(f) \mid \hat{T}_p \quad \text{if } p \parallel m \\ mf \mid \hat{T}_l \hat{T}_p - mpf \mid \hat{R}_p \hat{T}_{l/p} & = pP_l(f) \mid \hat{T}_p - pP_{l/p}(f^{(p)}) \quad \text{if } p^2 \mid m. \end{cases}$$

If $p \mid h$, this equals $P_m(f)$ directly, using Corollary 3.24.

If $p \nmid h$, we note that the Fourier series of $(mf \mid \hat{T}_m)(z)$ has leading term q^{-m}, as desired; and by Theorem 3.16, it has invariance group $F(f)$. So it remains to show that it has no poles (modulo $(1/h)\Gamma_0(n \mid h) + e_1, e_2, \dots$) except at $z = \infty$. This is done by considering four cases as in Theorem 2.28. ∎

REFERENCES

[ACMS] D. Alexander, C. Cummins, J. McKay, and C. Simons, Completely replicable functions, *in* "Groups, Combinatorics, and Geometry, Durham, 1990," pp. 87–98, Cambridge Univ. Press, Cambridge, UK, 1992.

[Bor] R. Borcherds, Monstrous moonshine and monstrous Lie superalgebras, *Invent. Math.* **109** (1992), 405–444.

[CoN] J. H. Conway and S. P. Norton, Monstrous Moonshine, *Bull. London Math. Soc.* **11** (1979), 308–339.

[CuN] C. Cummins and S. Norton, Rational Hauptmoduls are replicable, preprint.

[Fer1] C. Ferenbaugh, The Genus Zero Problem for $n \mid h$-type groups, *Duke Math. J.* **72** (1993), 31–63.

[Fer2] C. Ferenbaugh, Lattices and generalized Hecke operators, *in* "Proceedings, Monster Conference, Ohio State University, May 1993," to appear.

[FMN] D. Ford, J. McKay, and S. Norton, More on replicable functions, *Comm. Algebra* **22** (1994), 5175–5193.

[Kob] N. Koblitz, "Introduction to Elliptic Curves and Modular Forms," Springer-Verlag, Berlin/New York, 1984.

[Koi] M. Koike, On replication formula and Hecke operators, preprint.

[Ser] J. P. Serre, "A Course in Arithmetic," Springer-Verlag, Berlin/New York, 1977.